

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

- 1 1. A method for communicating cryptographic data through multiple
2 network layers, comprising:
3 receiving the cryptographic data at a node;
4 dividing the cryptographic data into multiple pieces; and
5 encapsulating different pieces of the cryptographic data in fields
6 associated with different network layers of a protocol stack in a data packet,
7 ~~whereby wherein the~~ cryptographic data ~~that is too larger than to be~~
8 ~~communicated in a single field can be, and wherein the cryptographic data is~~
9 ~~encapsulated within~~ communicated through multiple fields associated with
10 different network layers of the protocol stack.
- 1 2. The method of claim 1, wherein receiving the cryptographic data
2 involves performing at least one non-reversible function on a piece of input data
3 to produce the cryptographic data.
- 1 3. The method of claim 2, wherein the input data includes a public
2 key associated with the node.
- 1 4. The method of claim 2, wherein the input data includes a static
2 identifier associated with the node.
- 1 5. The method of claim 2, wherein an IPv6 address field of the data
2 packet is comprised of a 64-bit prefix followed by the most-significant 64 bits of

3 the output of the non-reversible function, and wherein a universal/local bit and an
4 individual/group bit of the IPv6 address are both set to "0".

1 6. The method of claim 5, wherein a SIP Call-ID field of the data
2 packet is comprised of a local-id and a host address, wherein
3 the local-id is comprised of the least-significant 128 bits of the output of
4 the non-reversible function; and wherein
5 the host address is comprised of the IPv6 address.

1 7. The method of claim 2, wherein an SSH public-key fingerprint
2 field of the data packet is comprised of the least-significant 128 bits of the output
3 of the non-reversible function.

1 8. The method of claim 2, wherein a MAC address field of the data
2 packet is comprised of the least-significant 64 bits of the output of the non-
3 reversible function.

1 9. The method of claim 2, wherein a JXTA Peer-ID field of the data
2 packet is comprised of the least-significant 128 bits of the output of the non-
3 reversible function.

1 10. The method of claim 2, wherein a JXTA Group-ID field of the data
2 packet is comprised of the least-significant 128 bits of the output of the non-
3 reversible function.

1 11. An apparatus for communicating cryptographic data through
2 multiple network layers, comprising:
3 a receiving mechanism configured to receive the cryptographic data at a
4 node;

5 a dividing mechanism configured to divide the cryptographic data into
6 multiple pieces; and
7 an encapsulation mechanism configured to encapsulate different pieces of
8 the cryptographic data in fields associated with different network layers of a
9 protocol stack in a data packet, ~~whereby wherein~~ the cryptographic data ~~that is too~~
10 ~~larger than to be communicated in~~ a single field, and wherein the cryptographic
11 data can be communicated through is encapsulated within multiple fields
12 associated with different network layers of the protocol stack.

1 12. The apparatus of claim 11, wherein the receiving mechanism is
2 configured to perform at least one non-reversible function on a piece of input data
3 to produce the cryptographic data.

1 13. The apparatus of claim 12, wherein the input data includes a public
2 key associated with the node.

1 14. The apparatus of claim 12, wherein the input data includes a static
2 identifier associated with the node.

1 15. The apparatus of claim 12, wherein an IPv6 address field of the
2 data packet is comprised of a 64-bit prefix followed by the most-significant 64
3 bits of the output of the non-reversible function, and wherein a universal/local bit
4 and an individual/group bit of the IPv6 address are both set to "0".

1 16. The apparatus of claim 15, wherein a SIP Call-ID field of the data
2 packet is comprised of a local-id and a host address, wherein
3 the local-id is comprised of the least-significant 128 bits of the output of
4 the non-reversible function; and wherein
5 the host address is comprised of the IPv6 address.

1 17. The apparatus of claim 12, wherein an SSH public-key fingerprint
2 field of the data packet is comprised of the least-significant 128 bits of the output
3 of the non-reversible function.

1 18. The apparatus of claim 12, wherein a MAC address field of the
2 data packet is comprised of the least-significant 64 bits of the output of the non-
3 reversible function.

1 19. The apparatus of claim 12, wherein a JXTA Peer-ID field of the
2 data packet is comprised of the least-significant 128 bits of the output of the non-
3 reversible function.

1 20. The apparatus of claim 12, wherein a JXTA Group-ID field of the
2 data packet is comprised of the least-significant 128 bits of the output of the non-
3 reversible function.

1 21. A computer system for communicating cryptographic data through
2 multiple network layers, comprising:
3 a central processing unit;
4 a semiconductor memory;
5 a receiving mechanism configured to receive the cryptographic data at a
6 node;
7 a dividing mechanism configured to divide the cryptographic data into
8 multiple pieces; and
9 an encapsulation mechanism configured to encapsulate different pieces of
10 the cryptographic data in fields associated with different network layers of a
11 protocol stack in a data packet;
12 ~~whereby wherein the cryptographic data that is too larger than to be~~
13 ~~communicated in a single field, and wherein the cryptographic data can be~~

14 | ~~communicated through~~ is encapsulated within multiple fields associated with
15 | different network layers of the protocol stack.

1 22. The computer system of claim 21, wherein the receiving
2 mechanism is configured to perform at least one non-reversible function on a
3 piece of input data to produce the cryptographic data.

1 23. The computer system of claim 22, wherein the input data includes
2 a public key associated with the node.

1 24. The computer system of claim 22, wherein the input data includes
2 a static identifier associated with the node.

1 25. The computer system of claim 22, wherein an IPv6 address field of
2 the data packet is comprised of a 64-bit prefix followed by the most-significant 64
3 bits of the output of the non-reversible function, and wherein a universal/local bit
4 and an individual/group bit of the IPv6 address are both set to "0".

1 26. The computer system of claim 25, wherein a SIP Call-ID field of
2 the data packet is comprised of a local-id and a host address, wherein
3 the local-id is comprised of the least-significant 128 bits of the output of
4 the non-reversible function; and wherein
5 the host address is comprised of the IPv6 address.

1 27. The computer system of claim 22, wherein an SSH public-key
2 fingerprint field of the data packet is comprised of the least-significant 128 bits of
3 the output of the non-reversible function.

1 28. The computer system of claim 22, wherein a MAC address field of
2 the data packet is comprised of the least-significant 64 bits of the output of the
3 non-reversible function.

1 29. The computer system of claim 22, wherein a JXTA Peer-ID field
2 of the data packet is comprised of the least-significant 128 bits of the output of
3 the non-reversible function.

1 30. The computer system of claim 22, wherein a JXTA Group-ID field
2 of the data packet is comprised of the least-significant 128 bits of the output of
3 the non-reversible function.

1 31. A method for verifying a data packet containing cryptographic
2 data, comprising:
3 receiving the data packet;
4 extracting pieces of cryptographic data from fields associated with
5 different network layers of a protocol stack within the data packet, wherein the
6 cryptographic data is larger than a single field, and wherein the cryptographic
7 data is encapsulated within multiple fields; and
8 verifying that each piece of extracted cryptographic data matches with a
9 corresponding portion of a piece of previously obtained cryptographic data.

1 32. The method of claim 31, wherein the previously obtained
2 cryptographic data is obtained through a process that involves performing at least
3 one non-reversible function on a piece of input data to produce the cryptographic
4 data.

1 33. An apparatus for verifying a data packet containing cryptographic
2 data, comprising:
3 a receiving mechanism configured to receive the data packet;
4 an extracting mechanism configured to extract pieces of cryptographic
5 data from fields associated with different network layers of a protocol stack

6 | within the data packet, wherein the cryptographic data is larger than a single field,
7 | and wherein the cryptographic data is encapsulated within multiple fields; and
8 | a verification mechanism configured to verify that each piece of extracted
9 | cryptographic data matches with a corresponding portion of a piece of previously
10 | obtained cryptographic data.

1 | 34. The apparatus of claim 33, wherein the previously obtained
2 | cryptographic data is obtained through a process that involves performing at least
3 | one non-reversible function on a piece of input data to produce the cryptographic
4 | data.

1 | 35. A computer system for verifying a data packet containing
2 | cryptographic data, comprising:
3 | a central processing unit;
4 | a semiconductor memory;
5 | a receiving mechanism configured to receive the data packet;
6 | an extracting mechanism configured to extract pieces of cryptographic
7 | data from fields associated with different network layers of a protocol stack
8 | within the data packet, wherein the cryptographic data is larger than a single field,
9 | and wherein the cryptographic data is encapsulated within multiple fields; and
10 | a verification mechanism configured to confirm that each piece of
11 | extracted cryptographic data matches with a corresponding portion of a piece of
12 | previously obtained cryptographic data.

1 | 36. The computer system of claim 35, wherein the previously obtained
2 | cryptographic data is obtained through a process that involves performing at least
3 | one non-reversible function on a piece of input data to produce the cryptographic
4 | data.